De Wbp en personeelsverwerkingen

Een ondergeschoven kindje bij compliance onderzoeken

Jeroen van Puijenbroek

In Nederland is de bescherming van persoonsgegevens sinds 1 september 2001 geregeld in de Wet Bescherming Persoonsgegevens (Wbp)[1]. Deze wet, die strekt tot uitvoering van Richtlijn 95/46/EG[2], stelt eisen aan de wijze waarop organisaties mogen omgaan met persoonsgegevens. Vrijwel alle private en publieke organisaties verwerken persoonsgegevens en hebben dus te maken met de Wbp. De Wbp is een kaderwet waarin de algemene privacybescherming[3] is geregeld. Daarnaast is er de nodige specifieke wet- en regelgeving, die eveneens van invloed is op de wijze waarop persoonsgegevens mogen worden verwerkt.

Inleiding

In organisaties gaat, zowel bij de implementatie van de Wbp als bij compliance-onderzoeken naar de naleving van de Wbp (oftewel privacy audits), de aandacht vooral uit naar de gegevensverwerkingen ten behoeve van de primaire processen en minder naar de verwerkingen ten behoeve van beheer en personeel.
Een veelgehoorde reden hiervoor is dat het risico van (imago)schade het grootst wordt geacht bij de verwerkingen ten behoeve van de primaire processen. Enerzijds omdat klanten, patiënten, et cetera bij privacyschendingen eerder de publiciteit zoeken (lees: met hun klacht naar *De Telegraaf* gaan) of naar de rechter stappen om schadevergoeding te eisen dan werknemers. Anderzijds omdat het College bescherming persoonsgegevens (Cbp) haar openlijk een boete oplegt omdat de verwerking niet is aangemeld. In tegenstelling tot verwerking ten behoeve van de primaire processen hoeven verwerkingen ten behoeve van beheer en personeel veelal niet te worden aangemeld. Een andere belangrijke reden waarom bij privacy audits weinig aandacht wordt besteed aan verwerkingen ten behoeve van beheer en personeel, is het feit dat organisaties het idee hebben dat de verwerkingen die vrijgesteld zijn van aanmelding, zoals de meeste personeelsverwerkingen, eenvoudige verwerkingen zijn waarvoor op Wbp-gebied weinig tot niets hoeft te worden geregeld.
In dit artikel wordt eerst kort ingegaan op de Wbp; we geven antwoord op de vraag wanneer deze wet van toepassing is, en hoe de wet is opgebouwd. Daarna zal het door het Cbp gepubliceerde document ‘Contouren voor compliance. Handreiking bij de Raamwerk Privacy Audit’ (hierna kortweg de Handreiking genoemd) worden besproken. Ten slotte wordt commentaar gegeven op de Handreiking zelf en zal aan de hand van de Handreiking worden aangegeven dat personeelsverwerkingen Wbp-technisch niet zo eenvoudig zijn, dat ze niet altijd voldoen aan de Wbp en dat daardoor het risico op (imago)schade ook bij dit soort verwerkingen aanwezig is.

Mr. Drs. J.P.M. van Puijenbroek RE is werkzaam als senior beleidsmedewerker Wbp bij Bureau Secretaris Generaal van het Ministerie van Justitie. Daarvoor was hij werkzaam als project manager bij Ernst & Young EDP audit. De auteur heeft dit artikel op persoonlijke titel geschreven.

Wbp

Organisaties hebben met een veelheid aan privacyregels te maken. De Wbp vormt de belangrijkste bron van privacyregels. Uitgangspunt van de Wbp is dat er in beginsel geen belemmeringen gelden voor de verwerking van persoonsgegevens zolang het maar op de juiste manier gebeurt. Volgens de Eerste Kamer moet deze wet worden gelezen als een wettelijk systeem waarin de rechten en

belangen van de verantwoordelijke en de rechten en de belangen van de betrokkene zich op evenredige manier dienen te verhouden[5], ook wel aangeduid met het evenwichtsbeginsel waarop de Wbp is gebaseerd.
De 'verantwoordelijke' is op grond van de Wbp degene die het doel en de middelen vaststelt voor de verwerking van de persoonsgegevens. In geval van de overheid moet het relevante bestuursorgaan als verantwoordelijke worden aangemerkt; op rijksniveau zijn dit de afzonderlijke ministers. Binnen de particuliere sector is verantwoordelijkheid belegd op het niveau van de rechtspersoon (directeur/directie) of de natuurlijke persoon bij een eenmanszaak. De 'betrokkene' is degene op wie een persoonsgegeven betrekking heeft, bijvoorbeeld de werknemers in geval van een personeelsadministratie. In tabel 5 aan het einde van dit artikel zijn de belangrijkste begrippen uit de Wbp gedefinieerd.

Toepassingsbereik

De Wbp is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet-geautomatiseerde verwerking. Om vast te stellen dat er sprake is van een verwerking van persoonsgegevens moet dus aan drie criteria worden voldaan, namelijk:

1. Het moet gaan om een *persoonsgegeven*.
2. Het moet gaan om een *verwerking*.
3. De verwerking moet *geheel of gedeeltelijk geautomatiseerd* zijn of ze zijn bestemd om te worden opgenomen in een *bestand*. Aangezien onder verwerking 'een handeling of geheel van handelingen' wordt verstaan, kan er ook sprake zijn van een combinatie van handmatige en geautomatiseerde handelingen die als één verwerking worden beschouwd, bijvoorbeeld een geautomatiseerde personeelsadministratie plus het papieren personeelsdossier. Het werkterrein van de EDP-auditor bestaat normaliter uit (deels) geautomatiseerde verwerkingen.

Een aantal gegevensverwerkingen valt niet binnen de reikwijdte van de Wbp. De Wbp is niet van toepassing op gegevensverwerkingen die voor persoonlijk of huiselijk gebruik zijn bestemd. Daarnaast is de Wbp niet van toepassing op een aantal wetten over gegevensverwerkingen waarvoor een eigen privacyregime geldt[6]. Een uitzondering wordt ook gemaakt voor verwerkingen met uitsluitend journalistieke, artistieke en literaire doeleinden.

Systematiek

De Wbp is, naast een gedeelte over toezicht en sancties, grofweg te verdelen in materiële normen en in meer formele normen (waarborgnormen).

Materiële normen
Hoofdstuk 2 van de Wbp, getiteld 'Voorwaarden voor de rechtmatigheid van persoonsgegevens', bevat de materiële normen van het privacyrecht (kwaliteitseisen die moeten worden gesteld aan de verwerking) en geldt als toetsingskader om vast te kunnen stellen of een verwerking rechtmatig is of niet. In dit hoofdstuk zijn bepalingen opgenomen ten aanzien van:

- verwerking in overeenstemming met de wet;
- behoorlijke en zorgvuldige gegevensverwerking;
- doelbinding;
- rechtmatige grondslag;
- verenigbaar gebruik;
- bewaartermijnen;
- kwaliteit van gegevens;
- vertrouwelijkheid;
- beveiliging;
- relatie bewerker - verantwoordelijke;
- verbod op verwerking van bijzondere gegevens;
- uitzonderingen op het verbod verwerking van bijzondere gegevens.

Een schending van bovenstaande materiële normen doet afbreuk aan de kwaliteit van de verwerking (ook wel aangeduid als privacyschending). De betrokkene wordt hierdoor benadeeld (schade). De schade kan leiden tot aansprakelijkheid van de verantwoordelijke.

Waarborgnormen
De artikelen over aanmelding (hoofdstuk 4), informatieverstrekking aan de betrokkene (hoofdstuk 5) en de rechten van de betrokkene (hoofdstuk 6) hebben in tegenstelling tot hoofdstuk 2 een formeler karakter. Zij voegen niets toe aan de kwaliteit van de verwerking als zodanig, maar waarborgen de naleving van de materiële normen. De waarborgnormen stellen de betrokkene in staat om zelfstandig vast te stellen of de verantwoordelijke zijn persoonsgegevens conform de privacywetgeving verwerkt. Hoewel de waarborgfunctie een wezenlijk onderdeel is van het privacyrecht, rijst de vraag of een schending van waarborgnormen even zwaar weegt als een schending van de materiële normen. Met andere woorden: kan iedere inbreuk op een voorschrift worden aangeduid als een privacyschending? Strikt genomen luidt het antwoord 'ja'. De woorden '… in overstemming met de wet…' in artikel 6 van de Wbp impliceert dat iedere wettelijke overtreding een onrechtmatige verwerking oplevert, dus ook een overtreding van een waarborgnorm.

Handreiking bij het Raamwerk Privacy Audit

De bescherming van persoonsgegevens is een verantwoordelijkheid van alle organisaties die met persoonsgegevens omgaan. Het Cbp stimuleert zelfregulering van overheid en bedrijfsleven voor een adequate privacybescherming onder andere door compliance-instrumenten

te (laten) ontwikkelen; instrumenten die gebruikt kunnen worden als handreiking voor het naleven van de geldende wet- en regelgeving.
Het Cbp heeft in samenwerking met het NIVRA en de NOREA in mei 2005 de 'Contouren voor Compliance. Handreiking bij het Raamwerk Privacy Audit' uitgebracht[7]. Naast de Handreiking zijn drie zelfreguleringsproducten ontwikkeld[8], te weten:

- de Quickscan;
- de Wbp-zelfevaluatie;
- het Raamwerk Privacy audit.

De Handreiking sluit aan bij het Raamwerk Privacy Audit[9] en ZekeRE Privacy[10] van de NOREA. Het is een hulpmiddel bij het concretiseren van de open normen van de Wbp. Bij de beoordeling, die betrekking heeft op één specifieke benoemde verwerking van persoonsgegevens, wordt gewerkt met een systeem van (straf)punten. Het aantal punten is afhankelijk van de vastgestelde risicoklasse en van de ernst van de afwijking. Aan de hand van het totaaloverzicht verwerkingen (zie tabel 1) worden de belangrijkste begrippen besproken.

Totaal Verwerkingseisen		Vooronderzoek Potentiële bevinding	Compliance onderzoek Feitelijke bevinding								
		Non-conformiteit	Non-conformiteit	Deficiëntie				Incident			
				Per risicoklasse							
				0	I	II	III	0	I	II	III
V.1 Voornemen en melden	Aantal deficiënties/ incidenten										
V.2 Transparantie	Aantal deficiënties/ incidenten										
V.3 Doelbinding	Aantal deficiënties/ incidenten										
V.4 Rechtmatige grondslag	Aantal deficiënties/ incidenten										
V.5 Kwaliteit	Aantal deficiënties/ incidenten										
V.6 Rechten van de betrokkene	Aantal deficiënties/ incidenten										
V.7 Beveiliging	Aantal deficiënties/ incidenten										
V.8 Verwerking door een bewerker	Aantal deficiënties/ incidenten										
V.9 Gegevensverkeer met landen buiten de EU	Aantal deficiënties/ incidenten										
			Totaal								
Gewicht deficiëntie / incident				**1**	**2**	**4**	**8**	**1**	**1**	**2**	**3**
			Aantal x gewicht:								
Op basis van het aantal van 33 aandachtsgebieden bij de negen verwerkingseisen voor persoonsgegevens bedraagt het maximale aantal '(straf)punten':				**33**	**66**	**132**	**264**	**33**	**33**	**66**	**99**

Tabel 1. Rekenmodel Totaal verwerkingseisen (uit: Contouren voor Compliance. Handreiking bij het Raamwerk Privacy Audit)

Verwerkingseisen

De materiële en waarborgnormen uit de Wbp zijn geclusterd naar negen gebieden, verwerkingseisen genoemd (zie tabel 1). De negen verwerkingseisen worden hieronder kort toegelicht, de opgenomen teksten zijn citaten uit het Raamwerk Privacy Audit.

V.1 Voornemen en melden
Binnen de organisatie worden persoonsgegevens verwerkt waarop de Wbp van toepassing is. Dit feit moet gemeld worden bij het Cbp of bij de functionaris voor de gegevensbescherming (FG). De FG is de onafhankelijke interne toezichthouder.

V.2 Transparantie
De betrokkene moet op de hoogte zijn van wat er met zijn persoonsgegevens wordt gedaan. Hij moet hierover worden geïnformeerd.

V.3 Doelbinding
Persoonsgegevens worden slechts voor een vooraf bepaald doel verzameld. Deze gegevens kunnen voor dat doel worden verwerkt en onder voorwaarden voor andere doelen.

V.4 Rechtmatige grondslag
Persoonsgegevens mogen alleen worden verzameld en verwerkt wanneer de grondslag daarvoor in de Wbp kan worden gevonden. Voor bijzondere persoonsgegevens gelden specifieke regels.

V.5 Kwaliteit
De verwerking van persoonsgegevens moet voldoen aan kwaliteitseisen. Kwaliteit betekent dat de persoonsgegevens toereikend, terzake dienend, niet bovenmatig, juist en nauwkeurig zijn gelet op de doeleinden waarvoor ze worden verzameld of vervolgens verwerkt.

V.6 Rechten van de betrokkene
Personen over wie gegevens worden verzameld hebben een aantal rechten, waaronder het recht op inzage, correctie, verwijdering, afscherming en verzet.

V.7 Beveiliging
Het Cbp heeft een apart document ontwikkeld, getiteld 'Beveiliging van persoonsgegevens'[BLAR01], waarin een normatief kader is uitgewerkt dat volgt uit artikel 13 van de Wbp. Hierin zijn de te nemen maatregelen, afhankelijk van de onderkende risicoklassen van persoonsgegevens, gegroepeerd in 14 categorieën.

V.8 Verwerking door een bewerker
De verantwoordelijke kan (een deel van) de verwerking van persoonsgegevens uitbesteden aan een bewerker. Dit moet worden vastgelegd in een overeenkomst of een andere rechtshandeling zodat er een verbintenis ontstaat tussen de bewerker en de verantwoordelijke.

V.9 Gegevensverkeer met landen buiten de EU
Indien er sprake is van gegevensverkeer met landen buiten de Europese Unie (EU) dan moet in het compliance-onderzoek worden gelet op de omstandigheden die op de doorgifte van gegevens of op een categorie gegevens van invloed zijn. In het bijzonder wordt rekening gehouden met de aard van de gegevens, met het doel of de doeleinden en met de duur van de voorgenomen verwerking of verwerkingen, het land van herkomst en het land van eindbestemming, de algemene en sectorale rechtsregels die in het betrokken derde land gelden, alsmede de regels van het beroepsleven en de veiligheidsmaatregelen die in die landen worden nageleefd.

Risicoklasse

Het begrip 'risicoklasse' is door het Cbp oorspronkelijk gedefinieerd voor het bepalen van het stelsel van maatregelen in het kader van de beveiliging van persoonsgegevens. Hierbij zijn vier risicoklassen onderkend, te weten:
- Risicoklasse 0: publiek niveau;
- Risicoklasse I: basisniveau;
- Risicoklasse II: verhoogd niveau;
- Risicoklasse III: hoog risico.

In tabel 2 is een schema opgenomen voor het bepalen van de risicoklasse.

Aard van de gegevens		Persoonsgegevens	Bijzondere persoonsgegevens Conform artikel 16 Wbp	Financieel en/of economische persoonsgegevens
Hoeveelheid persoonsgegevens per betrokkene)	Aard van de verwerking			
Weinig persoonsgegevens	Lage complexiteit van de verwerking	**Risicoklasse 0**	**Risicoklasse II**	**Risicoklasse II**
Veel persoons-gegevens	Hoge complexiteit van de verwerking	**Risicoklasse I**	**Risicoklasse III**	

Tabel 2. Schema voor het bepalen van de risicoklasse (uit:Beveiliging van Persoonsgegevens – AV23)

Voor het compliance-onderzoek (de privacy audit) is deze classificatie van toepassing verklaard op de gehele verwerking van persoonsgegevens, op alle negen verwerkingseisen. In de praktijk blijkt het classificeren van de verwerking niet eenvoudig te zijn. Op basis van de tabel en de gegeven toelichting in het document Beveiliging is het niet altijd mogelijk om een eenduidige keuze te maken tussen 'weinig' en 'veel' persoonsgegevens. De beoordeling van de hoeveelheid persoonsgegevens (veel/weinig) dient plaats te vinden per betrokkene, niet alleen op basis van het absolute aantal gegevens maar ook de verschillende soorten van gegevens.

Toleranties bij de beoordeling

Bij het beoordelen van een verwerking van persoonsgegevens zal de auditor de norm vergelijken met de aangetroffen situatie (vergelijking soll en ist-positie). Ten aanzien van aangetroffen verschillen wordt onderscheid gemaakt in drie situaties:
- *Non-conformiteit:* een structurele (stelselmatige), materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van een of meer betrokkene(n) in ernstige mate is of kan worden geschaad.
- *Deficiëntie:* een structurele (stelselmatige), niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van een of meer betrokkene(n) in niet ernstige mate is of kan worden geschaad.
- *Incident:* een incidentele, niet-materiële tekortkoming ten opzichte van de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes waardoor de bescherming van een of meer betrokkene(n) in niet ernstige mate is of kan worden geschaad.

Rekenmodel

Het model bestaat uit negen verwerkingseisen met per eis één of meerdere aandachtsgebieden, in totaal 33. Per aandachtsgebied moet worden bepaald of er sprake is van een non-conformiteit, deficiëntie en/of incident.
Een non-conformiteit leidt, ongeacht de risicoklasse van de verwerking, tot een negatief oordeel van de auditor; het beoordeelde stelsel voldoet niet aan de gestelde eisen.
Dit is de uitwerking van de woorden '… in overstemming met de wet…' in artikel 6 Wbp. Bij de systematiek van de Wbp is al aangegeven dat iedere wettelijke overtreding leidt tot een onrechtmatige verwerking; ongeacht of dit een overtreding van een materiële norm of waarborgnorm is.
Volgens de toelichting op het model is het aantal (straf)-punten voor elke deficiëntie of elk incident afhankelijk van de vastgestelde risicoklasse van de verwerking; een incident in een verwerking van persoonsgegevens met risicoklasse II leidt bijvoorbeeld tot twee (straf)punten (zie tabel 1).
Na afloop van het onderzoek worden alle punten opgeteld en is het aan de 'professional judgement' van de auditor om vast te stellen wat dit in totaliteit voor gevolgen heeft voor het uiteindelijke oordeel (positief of negatief).
Ten aanzien van het in de Handreiking opgenomen voorlopige rekenmodel (tabel 1) worden hieronder drie opmerkingen gemaakt.

1. In het huidige rekenmodel wordt, bij de berekening van het maximale aantal (straf)punten, uitgegaan van 33 aandachtsgebieden. Echter in de toelichting op het model gegevensverwerkingen is bij drie aandachtsgebieden aangegeven dat een tekortkoming op dat gebied altijd leidt tot een non-conformiteit.
   Dit betekent dat bij de berekening van het maximale

aantal '(straf)punten' niet moet worden uitgegaan van 33 gebieden maar van 30. In tabel 3 zijn de aangepaste maximale aantal (straf)punten opgenomen.

2. Het model gaat uit van een maximaal aantal (straf)punten dat is gebaseerd op het aantal aandachtsgebieden. Dit betekent dat in het model niet *elke* deficiëntie of *elk* incident per aandachtsgebied moet worden opgenomen, maar dat er deficiënties of dat er incidenten bij een bepaald aandachtsgebied voorkomen. Wanneer namelijk het daadwerkelijke aantal afwijkingen wordt opgenomen kan het aantal (straf)punten het maximale aantal overschrijden. In tabel 3 is de tekst over deficiënties/incidenten hierop aangepast.
3. Een privacy audit heeft betrekking op één verwerking of één geheel van verwerkingen. Voor deze verwerking of geheel van verwerkingen wordt één risicoklasse vastgesteld. In het huidige rekenmodel wordt het aantal aandachtsgebieden met een deficiëntie opgeteld, vermenigvuldigd met het gewicht (afhankelijk van de risicoklasse) en afgezet tegen het maximale aantal (straf)punten. Hetzelfde wordt ook gedaan voor de incidenten. Daar blijft het bij. Het toekennen van gewichten heeft alleen nut wanneer het aantal behaalde (straf)punten op grond van de deficiënties en de incidenten worden opgeteld en wordt afgezet tegen het totale aantal maximale strafpunten met betrekking tot de verwerkingseisen. In tabel 3 is deze aanvulling opgenomen.
   Een voorbeeld ter illustratie: bij een verwerking met risicoklasse II blijkt dat er bij zeven aandachtsgebieden deficiënties zijn aangetroffen en bij vijf aandachtsgebieden een of meer incidenten. Rekening houdend met de wegingen betekent dit dat er met betrekking tot deficiënties 28 (straf)punten zijn 'gescoord' uit een maximum van 120 en met betrekking tot incidenten 10 uit 60. Dit levert een totaal resultaat op van 38 punten uit een maximum van 180.

Totaal Verwerkings-eisen	Vooronderzoek Potentiële bevinding	Compliance onderzoek Feitelijke bevinding											
	Non-conformiteit	Non-conformiteit	Deficiëntie				Incident				Totaal			
			Per risicoklasse											
			0	I	II	III	0	I	II	III	0	I	II	III
V1. Aantal aandachtsgebieden met deficiënties /incidenten														
V9. Aantal aandachtsgebieden met deficiënties /incidenten														
Totaal														
Gewicht deficiëntie / incident			**1**	**2**	**4**	**8**	**1**	**1**	**2**	**3**				
Aantal x gewicht:														
Op basis van het aantal van 30 aandachtsgebieden bij de negen verwerkingseisen voor persoonsgegevens bedraagt het maximale aantal '(straf)punten':			**30**	**60**	**120**	**240**	**30**	**30**	**60**	**90**	**60**	**90**	**180**	**330**

Tabel 3 Aangepast Rekenmodel verwerkingseisen (deels weergegeven)

Op- en aanmerkingen Handreiking in relatie tot personeelsverwerkingen

Hieronder worden bij drie verwerkingeisen op- en aanmerkingen geplaatst. Deze hebben betrekking op de Handreiking zelf, de Handreiking in relatie tot personeelsverwerkingen of op actuele ontwikkelingen met betrekking tot deze verwerkingseisen. De verwerkingseisen zijn:

- V.1 Voornemen en melden;
- V.4 Rechtmatige grondslag;
- V.9 Gegevensverkeer met landen buiten de EU.

V.1 Voornemen en melden

Verplichte Melding bij Cbp voor het verkrijgen kwaliteitsoordeel

In het Raamwerk Privacy Audit bestaat deze verwerkingseis uit zes aandachtsgebieden. In de Handreiking worden door de scopeafbakening echter twee aandachtsgebieden als 'niet van toepassing' verklaard. Dit zijn de aandachtsgebieden 'Vaststellen van de aard van de verwerking en de verplichting tot melden' en 'Bijhouden van een centraal register'. Voor het verkrijgen van een kwaliteitsoordeel, bestemd voor het maatschappelijke verkeer, wordt namelijk als eis gesteld dat de verwerking bij het Cbp moet zijn aangemeld. Ook indien er voor de organisatie een Functionaris Gegevensbescherming (FG)[11] is benoemd waar de aanmelding zou kunnen plaatsvinden òf indien de verwerking is vrijgesteld van aanmelden[12].
Als voordelen van deze verplichte melding bij het Cbp worden genoemd:

- De afbakening wordt door de verantwoordelijke zelf opgesteld, waarbij het aan de auditor is om vast te stellen dat de aangetroffen verwerking van persoonsgegevens binnen die grenzen blijft.
- De belanghebbende bij het kwaliteitsoordeel kan in het openbare meldingenregister bij het Cbp vaststellen welke verwerking van persoonsgegevens is beoordeeld.

Het vereiste, dat zonder aanmelding bij het Cbp de verwerking geen kwaliteitsoordeel kan krijgen dat bestemd is voor het maatschappelijke verkeer, is een verzwaring ten opzichte van de wettelijke bepalingen.
De hiervoor genoemde argumenten zijn niet overtuigend. Zowel bij de aanmelding bij de FG alsook bij vrijgestelde verwerkingen, vindt namelijk een afbakening plaats door de verantwoordelijke. De melding bij de FG omvat dezelfde gegevens als die bij het Cbp. Om te kunnen vaststellen of een verwerking onder het Vrijstellingsbesluit Wbp[13] valt of meldingsplichtig is, moet de verantwoordelijke de verwerking op vijf aspecten vergelijken met de eisen uit het Vrijstellingsbesluit (zie tabel 4).
Eveneens kan in beide gevallen de belanghebbende vaststel-

len welke verwerking van persoonsgegevens is beoordeeld. De FG, moet net als het Cbp, een register bijhouden van de bij hen aangemelde gegevensverwerkingen die kosteloos moet kunnen worden geraadpleegd. Ten aanzien van de vrijgestelde verwerkingen moet de verantwoordelijke aan eenieder die daarom verzoekt nagenoeg dezelfde gegevens verstrekken als de gegevens die zij in het kader van de aanmelding aan het Cbp of de FG moet verstrekken (zie tabel 4).

Op grond van bovenstaande wordt voorgesteld om de scope de privacy audit niet te beperken tot alleen de bij het Cbp aangemelde verwerkingen. Dit zou ook betekenen dat de niet van toepassing verklaarde aandachtsgebieden alsnog bij de beoordeling moeten worden meegenomen. Hierdoor wordt een belangrijk inzicht verkregen over de wijze waarop de Wbp is geïmplementeerd in de organisatie: vindt al dan niet typering plaats van de verwerkingen en wordt er een centraal register bijgehouden en zo ja, wat staat daarin? Als auditor wil je toch kunnen controleren dat de organisatie zelf heeft vastgesteld of de verwerking is vrijgesteld en zo ja, op grond van welk artikel uit het Vrijstellingsbesluit.

Vrijgestelde verwerkingen
Als een organisatie persoonsgegevens verwerkt die overeenkomen met een van de soorten vrijgestelde gegevensverwerkingen wordt al snel aangenomen dat die verwerking daadwerkelijk ook onder het Vrijstellingsbesluit Wbp valt. De voor de verwerking verzamelde gegevens (nr. 1 t/m 5 uit tabel 4) moeten worden vergeleken met de eisen van het overeenkomstige soort verwerking uit het Vrijstellingsbesluit Wbp.
In de praktijk zie je regelmatig dat er op een of meer onderdelen wordt afgeweken van de vereisten uit het Vrijstellingsbesluit; bijvoorbeeld in de personeelsadministratie worden meer of andere gegevens verwerkt dan op grond van het Vrijstellingsbesluit is toegestaan of de gegevens worden aan andere ontvangers verstrekt dan in Vrijstellingsbesluit is opgenomen; bij videocameratoezicht worden bijvoorbeelden de bestanden langer bewaard dan de vermelde termijn in het Vrijstellingsbesluit. Dit zou betekenen dat deze verwerkingen alsnog moeten worden aangemeld.

Advies Cbp – Uitbreiding vrijstellingen in het kader van verlaging administratieve lastendruk
In het kader van de reductie van de administratieve lasten Wbp stelt het Cbp een uitbreiding voor van de vrijstellingen. Als argument wordt genoemd dat het bedrijfsleven de meldingsplicht ervaart als een zware administratieve last. Deze last zou veelal gelegen zijn in het feit dat de meldingsplicht de verantwoordelijke noodzaakt zijn gegevenshuishouding door te lichten en op orde te brengen.
Volgens het Cbp zou het uitbreiden van het Vrijstellingsbesluit voor het bedrijfsleven een besparing opleveren van ruim € 2 miljoen[14].
Op grond van het hierboven besprokene maakt het qua administratieve lasten voor de verantwoordelijke niet veel uit of een gegevensverwerking moet worden aangemeld of dat deze is vrijgesteld van aanmelding. Om te voldoen aan de Wbp zal een organisatie toch zijn gegevenshuishouding moeten doorlichten om vast te stellen of de persoonsgegevens die worden verwerkt, moeten worden aangemeld of niet (gegevens 1 t/m 5 uit tabel 4). Voor de aan te melden verwerkingen hoeven 'slechts' enkele aanvullende gegevens te worden verzameld (gegevens 6 en 7 uit tabel 4).

Gegevens noodzakelijk voor / Omschrijving gegevens	Vaststelling of verwerking is vrijgesteld van aanmelding (Vrijstellingsbesluit Wbp)	Aanmelding Cbp of FG (art. 28 lid 1 Wbp)	Inlichtingen verstrekking t.a.v. de vrijgestelde verwerkingen (art. 30 lid 3 Wbp)
1. Het doel of doeleinden van de verwerking	x	x	x
2. Een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben	x	x	x
3. De ontvangers of categorieën van ontvangers aan wie de gegevens wordenverstrekt	x	x	x
4. De voorgenomen doorgifte van gegevens naar landen buiten de Europese Unie	x	x	x
5. De periode gedurende welke de gegevens bewaart	x		
6. Een algemene beschrijving van de (voor)genomen maatregelen ter waarborging van de beveiliging van de verwerking om een voorlopig oordeel te kunnen geven		x	
7. Doel of doeleinden waarvoor de gegevens of categorieën van gegevens zijn of worden verzameld		x	

Tabel 4 Vergelijking te verzamelen gegevens in geval van vrijgestelde verwerking versus aan te melden verwerking

Naast het doorlichten van de informatiehuishouding, als reden voor de zware administratieve lasten van de meldingsplicht, werd ook het op orde brengen genoemd. Zoals hierboven al is aangegeven, heeft de vrijstelling alleen betrekking op de aanmeldingsplicht. Alle overige bepalingen van de Wbp moeten worden nageleefd.
Als de verwerking op orde moet worden gebracht, staat dat dus los van de meldingsplicht. Bovendien zouden organisaties voor het waarborgen van de betrouwbaarheid en continuïteit van de gegevensverwerking normaal gesproken al een stelsel van verwerkings- en beveiligingsmaatregelen moeten hebben getroffen. De privacybescherming leidt tot aanvullingen op dit stelsel van maatregelen en procedures. Wanneer organisaties aangegeven dat 'het op orde brengen' leidt tot zware administratieve lasten, zou moeten worden uitgezocht waar deze kosten betrekking op hebben. Hoofdzakelijk op het normale stelsel van verwerkings- en beveiligingsmaatregelen of hoofdzakelijk op de aan-

vullingen ten aanzien van de Wbp? In het eerste geval is er sprake van een oneigenlijk argument.
Het verschil aan administratieve lasten voor het bedrijfsleven tussen een aan te melden verwerking en een van aanmelding vrijgestelde aanmelding kan daarom niet zo heel groot zijn. Het door het Cbp vermelde bedrag van € 2 miljoen aan vermindering van administratieve lasten bij uitbreiding van het aantal vrijstellingen lijkt dan ook aan de hoge kant.

V.4 Rechtmatige grondslag

In overeenstemming met de wet

In artikel 6 van de Wbp is aangegeven dat de persoonsgegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze worden verwerkt. Aangezien het woord 'wet' in dit artikel niet alleen verwijst naar de Wbp, maar ook naar andere wetgeving inzake de verwerking van persoonsgegevens wordt in de Memorie van toelichting gesproken van een schakelbepaling. Een voorbeeld van een dergelijke andere wet is de hieronder opgenomen Wet op de Ondernemingsraad (WOR).
In de Handreiking is op meerdere plaatsen aangegeven dat bij de beoordeling van de gegevensverwerking niet alleen rekening moet worden gehouden met de eisen uit de Wbp, maar ook met die uit andere wet- en regelgeving. Echter in het model zelf komt deze eis vreemd genoeg niet expliciet terug bij de verwerkingseis 'Rechtmatige grondslag' (dit is evenmin het geval bij de verwerkingseis 'Kwaliteit'). Natuurlijk kan op voorhand niet voor elke situatie een norm worden gegeven om het kwaliteitsoordeel vast te stellen. Maar men zou toch mogen verwachten dat er bij de non-conformiteiten van deze verwerkingseisen een zin zou zijn opgenomen in de trant van 'De verantwoordelijke verwerkt persoonsgegevens conform de van toepassing zijnde wet- en regelgeving c.q. de daarvan afgeleide gedragscodes'. Deze zou dan door de auditor moeten worden ingevuld voor de concrete situatie. Door het opnemen van een algemene formulering wordt de kans kleiner dat de eisen uit andere wet- en regelgeving niet worden meegenomen bij het opstellen van het te hanteren normenkader.

Wbp en WOR

De Wbp stelt specifieke eisen aan de verwerking van persoonsgegevens. Daarnaast betreft het in bepaalde gevallen verwerkingen waarop de WOR van toepassing is.
De ondernemingsraad heeft instemmingsrecht indien de ondernemer een regeling vaststelt, wijzigt of intrekt met betrekking tot:

- de verwerking van personeelsgegevens (artikel 27 lid 1 onder k WOR);
- de toepassing van systemen die als personeelsvolgsystemen kunnen worden aangemerkt (artikel 27 lid 1 onder l WOR).

Instemming van de ondernemingsraad is dus niet alleen noodzakelijk voor regelingen met betrekking tot personeelsvolgsystemen zoals e-mail en internetcontrole of cameratoezicht op de werkplek, maar geldt voor alle regelingen met betrekkingen tot personeelsverwerkingen en systemen die gebruikt zouden kunnen worden als personeelsvolgsysteem. Dit laatste komt in wezen neer op alle geautomatiseerde systemen waarin de loggegevens van een medewerker worden opgeslagen; deze gegevens kunnen immers worden gebruikt voor productiviteitscontrole. In de visie van het Cbp is de melding van een verwerking een regeling als bedoeld in artikel 27 WOR. Mutatis mutandis geldt dit ook voor meldingen van vrijgestelde verwerkingen.
In de praktijk blijft het echter een lastige vraag: zijn er nu wel of geen regels waar het instemmingsrecht betrekking op heeft? En dan *kan* de volgende situatie zich voordoen: 'de ondernemingsraad wil instemming of beroept zich op artikel 27 WOR. De werkgever stelt dan dat er geen regels zijn en dat instemming dus niet nodig is. Vervolgens wendt de ondernemingsraad zich tot het Cbp en dan is het antwoord dat het niet hebben van regels over hoe moet worden omgegaan met personeelsgegevens niet behoorlijk en zorgvuldig is (artikel 6 Wbp), dus moeten er regels komen. Dan zijn we weer bij artikel 27 WOR en is de cirkel rond.'

Bij een compliance onderzoek naar verwerkingen van personeelsgegevens of personeelsvolgsystemen dan wel systemen die hiervoor geschikt zijn, moet de auditor in ieder geval vaststellen dat de ondernemingsraad instemming heeft verleend met de bij het Cbp of de FG aangemelde personeelsverwerkingen. De WOR is van toepassing op alle organisaties die vijftig of meer werknemers in dienst hebben .

Verwerkingsgrond

Elke gegevensverwerking moet gebaseerd zijn op ten minste een van de in de Wbp limitatief opgesomde verwerkingsgronden. Een van de verwerkingsgronden is de ondubbelzinnig verleende toestemming van de betrokkene. De Wbp stelt drie eisen aan toestemming:

- in vrijheid gegeven;
- gericht op een specifieke verwerking;
- geïnformeerd.

Gesteld kan worden dat in een afhankelijke relatie, zoals in een arbeidsrelatie, er geen sprake is van een in volledige vrijheid gegeven toestemming [TERS02]. In deze gevallen wordt dan ook gepleit voor het kwalificeren van toestemming als restgrond voor het verwerken van persoonsgegevens. De grondslag zal dan bijvoorbeeld gezocht moeten worden in het feit dat de gegevensverwer-

king noodzakelijk is in het kader van de bedrijfsvoering, in Wbp-termen 'noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke'.

V.9 Gegevensverkeer met landen buiten de EU

Persoonsgegevens mogen slechts naar een land buiten de EU, de zogenaamde derde landen[15], worden doorgegeven indien dat land een passend beschermingsniveau biedt. Voor een aantal landen heeft de Europese Commissie (EC) besloten dat een passend beschermingsniveau aanwezig is. De scope van een dergelijk besluit kan per land verschillen, deze landen zijn:

- Argentinië[16];
- Canada (voorzover het doorgifte betreft aan ontvangers onder de IPEDA (Information Protection and Electronic Documents Act). Onder 'ontvangers' verstaat de IPEDA organisaties in de particuliere sector die in het kader van commerciële activiteiten persoonsgegevens verzamelen, gebruiken of verstrekken)[17];
- Guernsey[18];
- Isle of Man[19];
- Verenigde Staten (voorzover a. de ontvangende partij de Safe Harbor Principles heeft onderschreven[20] of b. het doorgifte van het 'Passenger Name Record' van vliegtuigpassagiers betreft aan het Bureau of Customs and Border Protection van de Verenigde Staten[21]);
- Zwitserland[22].

Indien het betreffende derde land geen passende bescherming heeft, is doorgifte niet uitgesloten maar onderworpen aan aanvullende regels, onder andere:

- de betrokkene heeft daarvoor zijn ondubbelzinnige toestemming gegeven. Die toestemming moet wel van toepassing zijn op doorgifte naar het betrokken land;
- de doorgifte is noodzakelijk in het kader van een overeenkomst tussen u en de betrokkene. Als iemand bijvoorbeeld bij een bedrijf in een ander land een product bestelt, zullen de persoonsgegevens van de betrokkene naar het desbetreffende land moeten worden doorgegeven om die bestelling te kunnen uitvoeren. Daarvoor is dan geen afzonderlijke, ondubbelzinnige toestemming nodig.

Indien de toegestane uitzonderingsgronden niet toereikend blijken te zijn, kan de verantwoordelijke een vergunning aanvragen bij de minister van Justitie. Aan de vergunning worden nadere voorschriften verbonden die nodig zijn om de bescherming van de persoonlijke levenssfeer, alsmede de uitoefening van de daarmee verband houdende rechten te waarborgen. Deze waarborgen kunnen voortvloeien uit passende contractuele bepalingen die de verantwoordelijke in een overeenkomst opneemt met degene aan wie de gegevens worden doorgegeven.

De EC heeft drie modelcontracten ('standard contractual clauses') goedgekeurd die voldoende waarborgen bieden[23]. De aanvraag wordt ingediend bij het Cbp, zij voorziet de aanvraag van een advies en draagt het gehele dossier over aan de Dienst Justis van het Ministerie van Justitie, die namens de minister al dan niet een vergunning verleent. Indien de aanvrager gebruikmaakt van de door de Commissie goedgekeurde modelcontracten (zonder aanvullingen of wijzigingen) dan stelt het Cbp alleen vast of het contract correct, volledig en niet in tegenspraak met de Wbp is ingevuld.

Advies Cbp – Vrijstelling van vergunningsplicht bij gebruikmaking van modelcontracten

In 2003 heeft ondergetekende een kanttekening geplaatst bij de vergunningsplicht. Indien een verantwoordelijke gebruikmaakt van de door de Commissie goedgekeurde modelbepalingen, zijn er zoveel waarborgen getroffen dat er voor dit specifieke geval sprake is van een passend beschermingsniveau waardoor artikel 25 Richtlijn [artikel 76 Wbp] van toepassing is. Alleen in die gevallen dat wordt afgeweken van de modelcontracten dan wel deze worden aangevuld, zou een vergunning moeten worden aangevraagd bij de minister van Justitie [PUIJ03]. Sindsdien is het standpunt van het Cbp gewijzigd en heeft zij ondertussen de minister van Justitie geadviseerd om vrijstelling te verlenen voor de vergunningsplicht bij gebruikmaking van de modelcontracten[24].

Doorgifte personeelsgegevens naar derde landen

Voor doorgifte van personeelsgegevens naar landen buiten de EU kan in veel gevallen geen beroep worden gedaan op de toegestane uitzonderingsgronden. Hierboven is bij de opmerking over de rechtmatige verwerkingsgrond al aangegeven dat er in een arbeidsrelatie geen sprake kan zijn van een volledig in vrijheid gegeven toestemming. Dit is bij internationale gegevensuitwisseling problematisch omdat de verwerkingsgrond 'noodzakelijk voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke', als alternatief voor het geven van toestemming, niet als toegestane uitzonderingsgrond is opgenomen. Voor een rechtmatige doorgifte van personeelsgegevens betekent dit dat het vaak noodzakelijk is om een vergunning bij de minister van Justitie aan te vragen waarbij een van de modelcontracten als basis dient. Zowel het modelcontract, als de vergunning(aanvraag) zijn regelingen in de zin van artikel 27 WOR. Dit betekent dat de ondernemingsraad, net zoals bij de melding van de verwerking bij het Cbp of de FG, hierover instemmingsrecht heeft. Ook hier zal de auditor in het kader van een privacy audit moeten vaststellen dat de ondernemingsraad instemming heeft verleend.

Zoals hierboven is aangegeven controleert het Cbp – indien de verantwoordelijke ongewijzigd gebruikmaakt van het modelcontract – alleen of het contract correct, volledig en niet in tegenspraak met de Wbp is ingevuld. De meerwaarde van het Cbp bij de vergunningverlening zou juist moeten liggen in het feit dat ze in dit geval controleert of ook is voldaan aan de eisen uit specifieke wet- en regelgeving. Anders is de vergunningsplicht bij gebruikmaking van de modelcontracten inderdaad alleen maar een administratieve last die niet bijdraagt aan de gegevensbescherming na doorgifte.
Door in dit geval te controleren of voldaan is aan het instemmingsrecht op grond van de WOR kan worden voorkomen dat een ondernemingsraad bezwaar aantekent tegen een verleende vergunning voor doorgifte naar een derde land omdat zij geen instemming heeft gegeven. Of dat de ondernemingsraad naar de kantonrechter stapt omdat haar geen instemming is gevraagd. Dit kan leiden tot negatieve publiciteit waarop de verantwoordelijke niet zit te wachten.

Conclusie

Het model verwerkingseisen, zoals beschreven in de Handreiking, biedt de auditor nuttige handvatten voor het uitvoeren van een privacy audit. De scopeafbakening, dat alleen bij het Cbp aangemelde verwerkingen een kwaliteitsoordeel kunnen krijgen, is te beperkt. Ook bij de functionaris Gegevensbescherming aangemelde verwerkingen en van aanmelding vrijgestelde verwerkingen moeten een voor het maatschappelijk verkeer bestemd kwaliteitsoordeel kunnen krijgen. Daarnaast zal het rekenmodel op de aangegeven punten nog moeten worden aangepast, omdat anders het uiteindelijke oordeel (positief of negatief) dat de auditor neemt op grond van zijn 'professional judgement', gebaseerd is op onjuiste en/of onvolledige informatie. Bij het opstellen van het te hanteren normenkader dienen naast de eisen uit de Wbp ook eisen uit aanpalende wetgeving als normen te worden opgenomen. Dit stelt wel eisen aan de deskundigheid van de privacy-auditor, Het hebben van voldoende juridische en praktische kennis van de Wbp is onvoldoende. Dit blijkt ook wel uit de hierboven besproken complexe problematiek ten aanzien van de, op voorhand ogenschijnlijk eenvoudige, personeelsverwerkingen. Voor elke privacy-audit zal de auditor alle van toepassing zijnde sectorale wetgeving en gedragscodes in kaart moeten brengen en vaststellen in hoeverre deze (aanvullende) eisen stellen aan de verwerking van persoonsgegevens.
In de binnenkort te verschijnen ontwerprichtlijn 'Assurance-opdrachten met betrekking tot bescherming van persoonsgegevens (Privacy audits)' van het NIVRA en de NOREA wordt als eis gesteld dat de privacy-auditor naast de Wbp ook kennis moet hebben van overige relevante wet- en regelgeving waarbij wordt verwezen naar een bijlage. In deze bijlage komt de naleving van aanpalende wetgeving slechts summier terug.

Begrip	Omschrijving
Persoonsgegevens	Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.
Verwerking van persoonsgegevens	Elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in elk geval het verzamelen (het verkrijgen), vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
Bestand	Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
Verantwoordelijke	De natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Bewerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreekse gezag te zijn onderworpen.
Betrokkene	Degene op wie persoonsgegevens betrekking heeft.
Derde	Ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken.
Ontvanger	Degene aan wie de persoonsgegevens worden verstrekt (verstrekken is het bekend maken of het ter beschikking stellen van persoonsgegevens).
Bijzonder gegeven	Bijzondere persoonsgegevens zijn alle persoonsgegevens die informatie verschaffen over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging. Verder zijn bijzondere persoonsgegevens strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk handelen waarvoor een verbod is opgelegd (bijvoorbeeld een straatverbod).

Tabel 5. Begrippen Wbp

Literatuur

[BLAR01] Blarkom, G.W. van en J.J. Borking, (2001), Beveiliging van persoonsgegevens, in: Achtergrondstudies en verkenningen 23, Registratiekamer,april.

[PUIJ03] Puijenbroek, J.P.M. van, (2003), Gegevensverkeer met landen buiten de Europese Unie, in: Cuijpers, C.M.K. et al., Privacy concerns; het delen van persoonsgegevens bij fusies overnames en binnen concerns, Elsevier.

[TERS02] Terstegge, J.H.J., (2002), Wilt u hier even tekenen…? Betekenis van toestemming in het privacyrecht, in: Privacy & Informatie, nr. 4, augustus, pp. 157-162.

Noten

1 Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens, Staatsblad. 2000, 302.

2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995, PbEG 1995 L281/31.

3 Wanneer in dit artikel wordt gesproken over 'privacybescherming' wordt hiermee bedoeld de bescherming van de informationele privacy; bescherming van de persoonlijke levenssfeer in verband met het vastleggen van en verstrekken van persoonsgegevens (artikel 10 Grondwet).

4 Kamerstukken II 1997/1998, 25892, nr. 3, p. 20.

5 Kamerstukken I 1999/2000, 25 892, nr. 92c, p.16.

6 Wet op de inlichtingen en veiligheidsdiensten 2002, Politiewet 1993, Wet gemeentelijke basisadministratie persoonsgegevens, Wet justitiële en strafvorderlijke gegevens en Kieswet.

7 Cbp, NIVRA en NOREA, Contouren voor compliance. Handreiking bij het Raamwerk Privacyaudit, 24 mei 2005.

8 De Handreiking en de andere drie zelfreguleringsproducten zijn te downloaden via de site van het Cbp: (www.cbpweb.nl).

9 Samenwerkingsverband Audit-aanpak , 'Raamwerk privacy audit', 2001.

10 NOREA, ZekeRE privacy, 2002.

11 Een organisatie kan een eigen FG aanstellen. De taak van de FG is om op onafhankelijke wijze toezicht uit te oefenen op de organisatie. Instelling van een FG heeft tot gevolg dat meldingsplichtige gegevensverwerkingen niet meer bij het Cbp hoeven te worden gemeld maar bij de FG. Iedere verwerking moet, voordat daarmee wordt begonnen, worden gemeld bij het Cbp òf de FG.

12 In het Vrijstellingsbesluit Wbp zijn 42 veelvoorkomende soorten gegevensverwerkingen (o.a. sollicitatie, uitzendkrachten, personeelsadministratie, salarisadministratie, netwerksystemen, communicatieapparatuur, toegangscontrole en videocameratoezicht) opgenomen waarvan het bestaan in het algemeen mag worden verondersteld, en die daarom niet hoeven te worden aangemeld bij het Cbp of de FG.

13 Vrijstellingsbesluit Wbp, Staatsblad, 2001, 250.

14 Cbp, 10 voorstellen voor reductie administratie lasten Wbp, 7 december 1004 (kenmerk z2004-1086), p. 2.

15 Derde landen zijn alle landen buiten de Europese Unie met uitzondering met uitzondering van de landen van de Europese Economische Ruimte (EER). De landen van de EER (Noorwegen, Liechtenstein en IJsland) hebben zich verplicht Richtlijn 95/94/EG te implementeren in nationale wetgeving.

16 Beschikking C2003 1731, PbEG 2003 L 168.

17 Beschikking 2002/2/EG, PbEG 2002 L 2/13.

18 Beschikking 2003/821/EG, PbEG 2003 L 308/27.

19 Beschikking 2004/411/EG, PbEG 2004 L 151/1.

20 Beschikking 2000/520/EG, PbEG 2000 L 215/1.

21 Beschikking 2004/535/EG, PbEG 2004 L 235,11 en Besluit 2004/496/EG, PbEG, 2004 L183, 83.

22 Beschikking 2000/518/EG, PbEG 2000 L 215/1.

23 Beschikking 2001/497/EG, PbEG 2001 L 181/19: deze beschikking heeft betrekking op de doorgiften tussen twee verantwoordelijken waarvan er een binnen en een buiten de EU is gevestigd.
Beschikking 2002/16/EG, PbEG 2002 L6/52 (waar in de Wbp wordt gesproken van bewerker spreken de Europese Richtlijn en de daarop gebaseerde beschikkingen van verwerker): deze beschikking heeft betrekking op de doorgifte tussen een verantwoordelijke, gevestigd binnen de EU, en een bewerker, gevestigd buiten de EU.
Beschikking 2004/915/EG, PbEG 2004 L385/74: deze beschikking heeft betrekking op een door het bedrijfsleven opgesteld modelcontract voor de doorgifte tussen twee verantwoordelijken waarvan er één gevestigd is in een land binnen de EU en de andere partij buiten de EU gevestigd is.

24 Cbp, 10 voorstellen voor reductie administratie lasten Wbp, 7 december 1004 (kenmerk z2004-1086), p. 2.